Recepción de requerimientos y mockups

Contexto

Se reciben mockups validados con el cliente (ej. Claro para miniprogramas, o Koshka para backoffice). Cambios tardíos en requerimientos (como en el caso de Claro) generan retrabajo y retrasos en pruebas y entrega.

Tabla STRIDE

Categoría STRIDE	Amenaza identificada	Vulnerabilidad	Impacto potencial	Estrategia de mitigación
Spoofing	Envío de mockups o requerimientos falsos haciéndose pasar por el cliente.	Canales de comunicación no autenticados; ausencia de verificación del remitente.	Desarrollo sobre requisitos equivocados → retrabajo, costos y retrasos.	Usar canales autenticados (correo corporativo con SSO), firma digital de artefactos, y confirmación activa del cliente (workflow de aceptación).
Tampering	Alteración de mockups o especificaciones durante el tránsito o en almacenamiento temporal.	Transferencia por medios inseguros (email sin cifrado), almacenamiento en carpetas sin control de versiones.	Interpretación errónea de requisitos → pruebas inválidas y retrabajo.	Almacenar artefactos en repositorios seguros/versionados (p. ej. repositorio de requisitos o gestor de artefactos), uso de HTTPS/SFTP, checksums o firmas para verificar integridad.
Repudiation	El cliente niega haber aprobado cambios o nuevos mockups.	Ausencia de registro formal y sellado temporal de aprobaciones.	Disputas contractuales, alcance cambiante sin evidencia de aprobación.	Workflow de aceptación con firmas electrónicas y timestamps (p. ej. DocuSign, GitHub PR con aprobación del cliente/PO), registro inmutable de aprobaciones.
Information Disclosure	Exposición de información confidencial del cliente (contratos, pricing, mockups no publicados) por pérdida o acceso indebido.	Compartición por canales abiertos, o repositorios con permisos laxos.	Daño reputacional, pérdida de ventaja competitiva, incumplimiento contractual.	Clasificar la información, repositorios privados con control de acceso, cifrado en tránsito y en reposo, acuerdos de confidencialidad (NDA) con terceros.
Denial of Service	Retraso en aprobaciones por dependencia de un único aprobador o cuello de botella en el proceso de revisión.	Proceso de aprobación centralizado sin alternativas ni SLAs internos.	Paralización del inicio de pruebas, impacto en cronograma y fechas de entrega.	Establecer un Change Control Board (CCB), SLAs internos de respuesta, y múltiples aprobadores alternos autorizados.
Elevation of Privilege	Un actor no autorizado obtiene permisos para modificar/aprobar requisitos (ej. cuenta delegada sin control).	Falta de segregación de funciones y controles de acceso en la gestión documental.	Aprobaciones inválidas, cambios no autorizados que provocan retrabajo.	Implementar RBAC (roles claros), control de aprobadores autorizados, auditoría de cambios y revisión periódica de permisos.

Integración y pruebas funcionales (componentes modulares)

Contexto

Cada componente (frontend, backend, app móvil, Python embebido, OCPP, etc.) se valida de forma modular antes de integrarlo. En Thealth, por ejemplo, se prueban:

módulo BLE (conexión a ECG_ESP32), captura y almacenamiento de datos, ejecución local de cálculos en Python (Chaquo), visualización y exportación de resultados.

Tabla STRIDE

Categoría STRIDE	Amenaza identificada	Vulnerabilidad	Impacto potencial	Estrategia de mitigación
Spoofing	Dispositivo o componente falso (por ejemplo, un dispositivo BLE no autorizado) se hace pasar por uno legítimo durante la prueba.	Pairing/identificación débil entre dispositivos; falta de certificación de dispositivos de prueba.	Resultados de prueba inválidos, falsas alarmas o aprobaciones; riesgo de llevar configuraciones inseguras a producción.	Autenticación mutua (certificados o claves), pairing seguro, use de entornos de laboratorio con dispositivos registrados; lista blanca de dispositivos de prueba.
Tampering	Manipulación de paquetes de datos de prueba, artefactos de test o scripts de automatización.	Artefactos de prueba no verificables; almacenamiento de scripts sin control de integridad.	Resultados de pruebas corruptos; diagnósticos erróneos y decisiones equivocadas.	Firmar scripts/artefactos, checksums de resultados, almacenamiento seguro y controlado de artefactos de pruebas (artifactory), CI con verificación de integridad.
Repudiation	Un responsable niega haber ejecutado o aprobado una prueba que generó cambio en el código.	Falta de trazabilidad en la ejecución de pruebas y ausencia de registros con identidad.	Dificultad para asignar responsabilidad ante fallos; retrasos en corrección.	Registro de ejecuciones de pruebas asociado a usuarios (logs, pipeline IDs), commits y aprobaciones con firma (GPG), auditoría en CI/CD.
Information Disclosure	Exposición de datos sensibles capturados en pruebas (p. ej. señales biomédicas).	Uso de datos reales sin anonimizar; almacenamiento de datasets de prueba sin cifrar.	Violación de privacidad, riesgos regulatorios (GDPR/HIPAA), pérdida de confianza del cliente.	Anonimización/pseudonimización de datos, uso de datasets sintéticos, cifrado en reposo, políticas estrictas para acceso a datos de prueba.
Denial of Service	Pruebas que consumen recursos excesivos (p. ej. pruebas de carga sobre componentes sin aislamiento) provocan indisponibilidad del pipeline de pruebas.	Entornos compartidos sin límites de recursos; falta de mocks para dependencias pesadas.	Interrupción del pipeline de integración, retrasos en validación.	Entornos de pruebas aislados con cuotas, uso de mocks/stubs, limitación de pruebas paralelas, monitorización y alertas de recursos.
Elevation of Privilege	Código de prueba o paquetes de terceros ejecutados con permisos elevados en el entorno de test.	Entorno de pruebas con permisos demasiado amplios; ejecución de artefactos no verificados.	Compromiso del entorno de pruebas; posibilidad de propagación a entornos superiores.	Ejecutar pruebas en sandboxes, verificar y firmar paquetes de terceros, aplicar principio de menor privilegio en entornos de test.

Pruebas de interoperabilidad (flujo completo).

Contexto

Las pruebas de interoperabilidad validan el flujo completo entre componentes heterogéneos. Aquí se detectan errores de consistencia, sincronización en tiempo real y comportamientos emergentes entre sistemas.

Tabla STRIDE

Categoría STRIDE	Amenaza identificada	Vulnerabilidad	Impacto potencial	Estrategia de mitigación
Spoofing	Servicio, cliente o simulador se hace pasar por un componente legítimo en la integración (ej. un mock que acepta peticiones sin autenticación).	Autenticación inter-servicios insuficiente; uso de credenciales estáticas en pruebas.	Flujos integrados inválidos, fallos no detectados hasta producción.	Autenticación mTLS entre servicios, tokens con corta vida, emisión de certificados dedicados para entornos de prueba.
Tampering	Manipulación de payloads o mensajes en tránsito entre módulos (p. ej. alteración de pedido o de resultado de análisis).	Mensajes sin firma ni integridad verificada; uso de canales inseguros.	Inconsistencias de datos, errores funcionales y pérdida de confianza en resultados.	Firmado y encriptado de mensajes, validación de esquemas (JSON Schema), uso de bus de mensajes seguro.
Repudiation	Un módulo niega haber recibido o enviado un evento crítico que afectó el flujo (p. ej. actualización de inventario no registrada).	Falta de tracing distribuido y correlación de eventos.	Dificultad para diagnosticar fallos y conciliaciones, disputas entre equipos/partes.	Implementar tracing distribuido (OpenTelemetry), logs correlacionados y auditables, event sourcing donde aplique.
Information Disclosure	Datos sensibles (inventarios, métricas o señales biomédicas) expuestos entre sistemas o en logs.	Logs verbosos con datos sensibles; canales internos no cifrados.	Violaciones de privacidad, incumplimiento contractual y regulatorio.	Encriptación E2E, redacción de logs (no incluir PII), enmascaramiento de datos en logs, políticas de retención y acceso.
Denial of Service	Un módulo sobrecargando a otros (p. ej. burst de pedidos que colapsa backoffice).	Falta de rate limiting, retries agresivos y sin circuit breakers.	Interrupción del flujo completo, impacto en SLAs y pérdida de ingresos.	Implementar rate limiting, circuit breakers, backpressure y pruebas de resiliencia (chaos testing).
Elevation of Privilege	Servicio con token/configuración adquiere permisos más allá de lo necesario y puede manipular datos críticos.	Roles o scopes demasiado amplios para cuentas de servicio.	Acceso y modificación no autorizada de datos críticos, posible escalada a producción.	Principio de menor privilegio para cuentas de servicio, revisión periódica de scopes, uso de identidades gestionadas con rotación de credenciales.

Seguridad y cumplimiento

Contexto

En proyectos como Claro o Thealth, se requiere validar autenticación, autorización, protección de datos sensibles (ej. señales biomédicas) y cumplimiento contractual (SaaS, revenue share, reportes).

Tabla STRIDE

Categoría STRIDE	Amenaza identificada	Vulnerabilidad	Impacto potencial	Estrategia de mitigación
Spoofing	Robo de tokens o sesiones para suplantar usuarios/clientes.	Tokens de larga duración sin revocación; almacenamiento inseguro.	Acceso no autorizado a recursos y fuga de datos sensibles.	Tokens de corta vida, refresh seguro, revocación centralizada, almacenamiento de credenciales en gestores de secretos.
Tampering	Manipulación de reportes de revenue share o métricas contractuales.	Reportes sin firmas digitales ni controles de integridad.	Pérdidas económicas, disputas contractuales.	Firmado digital de reportes, registros inmutables (append-only), auditoría independiente.
Repudiation	Cliente/proveedor niega eventos (ej. facturación, entregas).	Logs incompletos o manipulables; falta de evidencia forense.	Disputas legales, incumplimiento de SLA.	Logs inmutables con timestamps, pruebas electrónicas de entrega y aceptación, blockchain o sistemas notarizados.
Information Disclosure	Fuga de datos biomédicos o métricas de negocio más allá de lo autorizado.	Almacenamiento en servicios no certificados o sin clasificación.	Multas regulatorias (GDPR/HIPAA), pérdida de confianza del cliente.	Clasificación de información, cifrado, data minimization, contratos que especifiquen servicios certificados.
Denial of Service	Ataques que impiden cumplimiento de SLA (infra caída, DB saturada).	Sin plan de continuidad ni mitigación DDoS.	Penalizaciones contractuales, daño reputacional.	Planes de continuidad, pruebas de carga, autoscaling seguro, mitigación DDoS.
Elevation of Privilege	Personal interno con acceso excesivo compromete datos críticos.	Roles y accesos mal definidos.	Acceso indebido a información sensible; incumplimiento de normativas.	Principio de menor privilegio, segregación de funciones, accesos JIT (Just In Time), revisiones periódicas de IAM.

Pruebas de Usuario (UAT)

Contexto

En UAT se entrega una versión controlada al cliente o grupo reducido de usuarios. Se mide rendimiento en dispositivos, usabilidad de interfaz y cumplimiento de métricas solicitadas. Ejemplo: HRV en Thealth.

Tabla STRIDE

Categoría STRIDE	Amenaza identificada	Vulnerabilidad	Impacto potencial	Estrategia de mitigación
Spoofing	Testers o clientes se hacen pasar por usuarios autorizados para acceder a builds preliminares.	Accesos compartidos o sin verificación estricta.	Fuga de builds privadas, exposición de funciones no liberadas.	Cuentas temporales para testers, MFA, validación previa de identidad.
Tampering	Testers modifican datos o manipulan builds, alterando resultados de pruebas.	Entornos de prueba no aislados; builds sin control de integridad.	Métricas falsas, dificultad para validar resultados reales.	Builds firmadas digitalmente, entornos UAT aislados, validación de integridad al inicio de

				la sesión.
Repudiation	Un tester niega haber aprobado/rechazado un entregable.	Falta de registros de sesiones de prueba y aprobaciones formales.	Disputas sobre aceptación del producto.	Evidencias de prueba (video, logs), aceptación formal con timestamp (ej. tickets firmados).
Information Disclosure	Uso de datos productivos en UAT expone información sensible.	Copia directa de bases de datos reales al entorno de prueba.	Violación de privacidad, multas regulatorias.	Uso de datos sintéticos o anonimización, control estricto de acceso a UAT.
Denial of Service	UAT consume recursos excesivos y afecta producción.	Infra compartida sin límites de recursos.	Caídas de servicios críticos durante validaciones.	Separación de entornos, quotas de recursos, escalamiento controlado para pruebas.
Elevation of Privilege	Tester obtiene permisos de administrador en UAT.	Roles y permisos mal configurados en el entorno.	Manipulación de pruebas, exposición de configuraciones sensibles.	Principio de menor privilegio, segregación de funciones en UAT, auditorías de accesos.

Entrega y despliegue controlado

Contexto

El despliegue nunca es directo a producción: primero staging, luego producción escalonada. Ejemplo: Claro valida en QA interno de Macondo y luego en su propio equipo antes de liberar en la SuperApp Mi Claro.

Tabla STRIDE

Categoría STRIDE	Amenaza identificada	Vulnerabilidad	Impacto potencial	Estrategia de mitigación
Spoofing	Solicitudes de despliegue fraudulentas o pipelines disparados por actores no autorizados.	Triggers de CI/CD no protegidos; accesos al repositorio sin MFA.	Despliegues no autorizados, caída del servicio.	Branches protegidos, MFA en CI/CD, aprobaciones manuales con firma digital, integración con SSO.
Tampering	Manipulación de builds entre el proceso de build y despliegue.	Artefactos no firmados, registries inseguros.	Código alterado en producción.	Firmado de artefactos, almacenamiento en registries seguros, validación de hashes al desplegar.
Repudiation	Negación de responsabilidad ante un despliegue fallido.	Falta de registros auditables en CI/CD.	Conflictos internos, retraso en correcciones.	Auditoría en pipelines, registro de aprobaciones con timestamp, releases taggeados y firmados.
Information Disclosure	Exposición de secretos (API keys, credenciales) en pipelines.	Variables de entorno sin protección; secrets en código.	Compromiso de servicios externos; fuga de datos.	Secret management (Vault, AWS Secrets Manager), cifrado de variables, prohibir secrets en repositorios.
Denial of Service	Despliegue interrumpe el servicio (errores en migraciones, config errónea).	Sin pruebas previas o rollback automático.	Downtime, incumplimiento de SLA.	Canary/blue-green deployments, staging previo, scripts de rollback automáticos.
Elevation of Privilege	Pipeline concede permisos excesivos a la aplicación en producción.	IAM permisivo para servicios.	Acceso indebido a datos y sistemas productivos.	Políticas IAM de mínimo privilegio, credenciales con scope limitado, revisiones periódicas.

Monitoreo post-entrega

Contexto

Tras la entrega, se habilitan logs y alertas en tiempo real. Ejemplo: en Macondo Food se asegura que MongoDB Atlas haga autoscaling; en Thealth se monitorean conexiones BLE y consumo de batería.

Tabla STRIDE

Categoría STRIDE	Amenaza identificada	Vulnerabilidad	Impacto potencial	Estrategia de mitigación
Spoofing	Agentes falsos envían métricas o logs fraudulentos.	Telemetría sin autenticación ni validación de origen.	Alarmas falsas o ceguera operacional.	Autenticación de agentes, firmas digitales en métricas, certificados para agentes válidos.
Tampering	Alteración o supresión de logs y métricas post-entrega.	Logs almacenados en sistemas modificables.	Pérdida de evidencia para auditoría y análisis forense.	Logs inmutables (append-only), almacenamiento seguro con control de acceso, replicación en sistemas externos.
Repudiation	Un equipo niega haber recibido o generado alertas críticas.	Falta de historiales verificables de alertas y eventos.	Disputas en RCA, incumplimiento de SLA.	Registro centralizado de alertas con sellos de tiempo, auditoría independiente, dashboards históricos.
Information Disclosure	Exposición de datos sensibles en logs de monitoreo (ej. datos biomédicos, información de clientes).	Logs verbosos con datos en claro.	Violación de privacidad, incumplimiento normativo.	Redacción/anonymización en logs, cifrado en tránsito y reposo, control de acceso basado en roles.
Denial of Service	Sobrecarga del sistema de monitoreo (exceso de métricas, spam de logs).	Falta de límites en ingesta de telemetría.	Saturación de sistemas de observabilidad, pérdida de visibilidad real.	Rate limiting en agentes, muestreo de métricas, almacenamiento escalable en la nube.
Elevation of Privilege	Acceso indebido a paneles de monitoreo o dashboards con permisos de administrador.	Roles mal configurados en sistemas de observabilidad.	Manipulación de métricas, ocultamiento de incidentes.	Configuración estricta de RBAC, separación de funciones, revisiones periódicas de accesos.

Gestión de tareas en Macondo

Contexto

El proceso de gestión de tareas se realiza de manera manual. Luego de la daily, la Scrum Master toma notas en papel y lápiz sobre las tareas acordadas. Después, transcribe esta información al tablero en GitHub para su seguimiento. Posteriormente, revisa la planificación con el líder técnico y asigna las tareas a cada miembro del equipo con sus cargas horarias, verificando además que se cumplan los SLA (Service Level Agreement) establecidos para el proyecto.

Tabla STRIDE

Categoría STRIDE	Amenaza Identificada	Vulnerabilidad	Impacto Potencial	Estrategia de Mitigación
Spoofing (Suplantación)	Alguien accede al tablero de GitHub con credenciales robadas y modifica las tareas.	Uso compartido de cuentas o contraseñas débiles.	Asignaciones incorrectas, pérdida de control sobre planificación.	MFA en GitHub, gestión individual de cuentas, políticas de contraseñas seguras.
Tampering (Alteración)	Manipulación de las notas al transcribirlas o alteración de tareas en GitHub.	Proceso manual no trazable, sin control de integridad.	Distorsión de acuerdos de la daily, retrasos en entregas.	Digitalizar la captura de la daily, mantener logs de cambios en GitHub.
Repudiation (Repudio)	Un miembro del equipo niega haber aceptado una tarea o compromiso de horas.	No existen registros firmados de la daily ni trazabilidad de asignaciones.	Conflictos internos, incumplimiento de SLA.	Registrar digitalmente acuerdos en la daily (ej. actas en herramientas colaborativas), usar comentarios en issues de GitHub con trazabilidad.
Information Disclosure (Divulgación de Información)	Pérdida, robo o acceso no autorizado al cuaderno físico con las notas de la daily.	Uso de medio manual sin cifrado ni control de acceso.	Exposición de acuerdos internos, SLA y planificación a terceros no autorizados.	Digitalizar las notas en una herramienta segura (ej. Confluence, Notion, GitHub Wiki), restringir acceso solo a miembros del equipo.
Denial of Service (DoS)	Inaccesibilidad al tablero en GitHub (caída, bloqueo de cuenta).	Dependencia total de una única plataforma.	Bloqueo en la gestión de tareas, retraso en entregas.	Mantener backups de tareas, plan de contingencia en otra herramienta.
Elevation of Privilege (Escalamiento de Privilegios)	Un miembro del equipo obtiene permisos de administrador en GitHub sin autorización.	Roles mal configurados en el repositorio.	Manipulación de asignaciones y datos críticos.	Principio de mínimo privilegio, revisión periódica de permisos en GitHub.